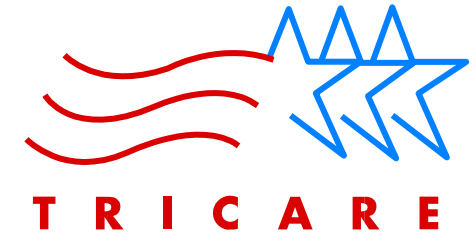
HEALTH AFFAIRS



TRICARE Management Activity

Personnel Trustworthiness Requirements for Access to DoD Information Technology (IT) Systems, Networks and Sensitive Data

April 2003

HEALTH AFFAIRS

T-RRx SOW
Personnel Security

TRICARE Management Activity

C.14.8 Information Systems (IS)/Networks Personnel Security. The contractor shall achieve the same level of trustworthiness of personnel who have access to IS/Networks involved in the operation of TRRx program systems of records as required for Government personnel requiring similar access to DoD information technology systems and networks containing sensitive information (SI) (See Appendix 6, DoD 5200.2-R, June 2002 (draft) Positions Requiring Access to DoD Information Technology (IT) Systems and Networks at http://www.tricare.osd.mil/tmis_new/ia.htm). To ensure the trustworthiness of personnel with access to DoD systems/data the contractor will classify Information Technology (IT) or related positions, submit appropriate paperwork for background investigations, ensure individuals receive requisite training, and document compliance. Personnel background investigations and training must be initiated before access to DoD IS/networks or DoD SI is allowed for operation of contractor IS/Networks. The website listed above will provide additional guidance to support this effort. All contractor employees with access to SI that is maintained in contractor owned and operated IT systems that have no interconnection (including data feeds) with Government IT systems or networks, shall complete the appropriate background check for IT-III level personnel comparable to that described in the referenced Appendix 6 to DoD 5200.2-R unless the contractor proposes, and the contracting officer approves, other alternative safeguards appropriate to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of the SI.

HEALTH AFFAIRS

Steps to Ensure Trustworthiness of Personnel

TRICARE Management Activity

- Contractors classify positions according to level of access required
- Contractors request the investigation based on position classification
- Contractors ensure personnel are appropriately trained
- Contractors ensure personnel understand and acknowledge their responsibilities

HEALTH AFFAIRS

Access to Need-to-Know Information

TRICARE Management Activity

Determine access level based on requirements of job:

Level of Access	Definition	IT Access Category
Privileged	Ability to alter any rules or controls of systems/networks, e. g., System Administrator	ADP/IT - I
Limited Privileged	Ability to alter some rules or controls of a single system or isolated network, e. g., Developer	ADP/IT - II
Non-privileged	No ability to alter any rules or controls, e. g., User	ADP/IT - III

HEALTH AFFAIRS

TRICARE

TRICARE Management Activity

Access to Information

- **The organization's security officer must request the proper IT investigation before granting access to systems/networks**
  - ADP/IT-I: SSBI
  - ADP/IT-II: NACLC
  - ADP/IT-III: NAC

SSBI - Single Scope Background Investigation
NACLC - National Agency Check With Local Agency Checks & Credit Checks
NAC - National Agency Check

- **Organization submits to OPM**
  - SF 85P, "Questionnaire for Public Trust Positions"
  - FD 258, "Fingerprint Card"
  - Credit check release for ADP/IT- I or II access

HEALTH AFFAIRS

Information Assurance Training

TRICARE Management Activity

- **Organization must ensure personnel receive training to perform IA responsibilities**
  - Security and information safeguarding
  - Incident Response
  - Configuration Management
  - Continuity of Operations or Disaster Recovery Plan
- **Training must be documented in individual personnel files**